

Secure MIMO Communications under Quantized Channel Feedback in the presence of Jamming

Theodoros Tsiligkaridis, *Member, IEEE*

Abstract—We consider the problem of secure communications in a MIMO setting in the presence of an adversarial jammer equipped with n_j transmit antennas and an eavesdropper equipped with n_e receive antennas. A multiantenna transmitter, equipped with n_t antennas, desires to secretly communicate a message to a multiantenna receiver equipped with n_r antennas. We propose a transmission method based on artificial noise and linear precoding and a two-stage receiver method employing beamforming. Under this strategy, we first characterize the achievable secrecy rates of communication and prove that the achievable secure degrees-of-freedom (SDoF) is given by $d_s = n_r - n_j$ in the perfect channel state information (CSI) case. Second, we consider quantized CSI feedback using Grassmannian quantization of a function of the direct channel matrix and derive sufficient conditions for the quantization bit rate scaling as a function of transmit power for maintaining the achievable SDoF d_s with perfect CSI and for having asymptotically zero secrecy rate loss due to quantization. Numerical simulations are also provided to support the theory.

Index Terms—Quantized CSI feedback, MIMO communication, linear precoding, Grassmann manifold, physical layer security, secrecy rate.

I. INTRODUCTION

Secrecy in the physical layer is concerned with maximizing the information rate of a transmitter-receiver pair such that reliable communication is possible, while keeping the information as private as possible if eavesdroppers listen. The seminal work of Wyner on the wiretap channel [1] has shown that it is possible to reliably communicate at a strictly positive rate while an eavesdropper listening to the transmitted signal through its own channel cannot decode the message. These results were generalized to Gaussian channels by Leung-Yan-Cheong and Hellman in [2] and to arbitrary broadcast channels by Csiszar and Korner in [3]. Following these important early works, various extensions to different system settings and assumptions have been made. Particularly, there has been considerable interest in studying physical layer secrecy for multiple-input multiple-output (MIMO) Gaussian channels, as the use of multiple antennas can increase secrecy capacity [4], [5]. In many works, the assumption of the transmitter knowing its channel to the eavesdropper is often impractical. As a

result, transmission strategies exploiting multiple antennas and injecting controlled artificial noise into the transmitted signal have been proposed in [6] in order to enhance secrecy.

Quantized feedback schemes have been proposed and studied in the literature for single user and multiple user down-link communication systems in [7], [8]. Motivated by the quantization approach of Rezaee & Guillaud [9], [10], which considered interference alignment for the MIMO interference channel with quantized channel feedback, we study the value of quantized feedback for secrecy communications in the presence of a hostile jammer. A key motivator for our work is the paper by Krishnamachari et al. [11], where a Grassmannian feedback scheme was studied in the context of interference alignment for MIMO interference channel. It was shown that if the feedback bit rate increases fast enough as a function of signal-to-noise ratio (SNR), the quantized channel estimates can be used at the transmitters to achieve the full multiplexing gain. However, communication under secrecy was not considered in these works on quantized CSI feedback. Optimal power allocation algorithms and achievable secrecy rates have been recently studied in the context of secrecy communications with artificial noise in [12], [13], but no degree-of-freedom (DoF) analysis is performed and perfect CSI is assumed. To the best of our knowledge, the value of quantized channel feedback on the secure DoF gain has not been studied in the literature in the context of communicating under secrecy and in the presence of a hostile jammer.

The transmission model that we consider consists of transmitting a linear combination of artificial noise and desired signal to a receiver. The purpose of the artificial noise is to confuse the eavesdropper and the desired signal is the signal to be decoded by the intended receiver. The artificial noise aspect has been studied in [6], [14], [15], [16]. In [6], the approach of transmitting artificial noise in the nullspace of the direct channel matrix was proposed assuming the number of transmit antennas, n_t , are more than the number of receive antennas, n_r . Thus, the designed artificial noise has no impact on the received signal at the intended receiver, but causes degradation at the eavesdropper thus enhancing secrecy. Robust beamforming for secure MIMO communications was studied in [15] under inaccurate CSI using a second-order perturbation analysis. The effect of delayed perfect CSIT on the SDoF gain was studied in [16] in the context of the two-user broadcast MIMO channel. In [14], the optimal power allocation among artificial noise and desired signal is derived such that the ergodic secrecy rate is maximized for a fixed number of feedback bits and transmit power. In addition, a scaling law between feedback bits and power is derived

Copyright (c) 2014 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Approved for Public Release, Distribution Unlimited.

T. Tsiligkaridis is with MIT Lincoln Laboratory, Lexington, MA 02421 USA (email: ttsili@ll.mit.edu).

to guarantee a constant secrecy rate loss compared to the perfect CSI case. Our work differs from these works since we derive explicit conditions for the quantization bit scaling that guarantee the optimal SDoF scaling, under similar assumptions on channel values as made in [11], and in addition we consider a jammer interfering with the received signal and show that the secrecy rate loss due to quantization is asymptotically negligible as SNR grows. Furthermore, our work differs from [14] because we consider quantization of a function of the direct channel matrix using (deterministic) quantization theory on the Grassmann manifold, adopt different channel conditions as adopted in [9], [10], [11] and thus, develop different proof techniques. In addition, the SDoF performance of artificial noise transmission schemes has not been studied in [6], and we also consider the lack of instantaneous perfect CSI by assuming the availability of quantized CSI. Our work differs from [15], [16] in that we consider a jammer and the effect of Grassmannian-based quantized instantaneous CSI on SDoF gain in a point-to-point MIMO channel.

In our problem formulation, the receiver's strategy is to null out the jammer interference and use its remaining resources to recover the information-bearing signal from the transmitter through beamforming. Under perfect CSI conditions, assuming $n_t > n_r$, the transmitter designs the artificial noise signal to lie in the nullspace of the channel matrix \mathbf{H}_d and the information-bearing signal to lie in the orthogonal complement of the null space of \mathbf{H}_d . Under this linear precoding strategy, the receiver sees no leakage due to artificial noise in the received signal. However, if the transmitter has imperfect CSI, then the received signal will contain a non-negligible amount of artificial noise. In the high SNR regime, this leakage will deteriorate the secrecy rate performance and drive the SDoF to zero. In order to maintain the full SDoF gain of the system, the rate of quantized feedback needs to increase appropriately as a function of SNR. In this paper, we characterize this rate and identify the key parameters associated with it. We also prove that, as the transmit power grows asymptotically, there is no loss in secrecy rate performance due to quantization.

A. Outline

The outline of this paper is as follows. Section II formulates the basic problem. Section III studies the achievable secrecy communication rates in the case of perfect CSI. Section IV studies the case of quantized CSI and derives performance bounds on the achievable secure degrees-of-freedom. The theory is illustrated by simulation in Section V and is followed by our conclusions in Section VI.

B. Notation

We use \mathbb{R} and \mathbb{C} to denote the real and complex fields. We use boldface lowercase letters \mathbf{x} to denote vectors and bold uppercase letters \mathbf{A} for matrices. Given a matrix $\mathbf{A} \in \mathbb{C}^{m \times n}$, we let \mathbf{A}^* denote its Hermitian conjugate, and \mathbf{A}^T denote its transpose. The trace operator $\text{tr}(\cdot)$ on a square matrix is simply the sum of its diagonal entries. Let $\text{Nul}(\mathbf{A})$ and $\text{Col}(\mathbf{A})$ denote the nullspace and column spaces (i.e., range) of the matrix \mathbf{A} .

We let $\mathcal{N}_c(\mu, \Sigma)$ denote the complex multivariate normal distribution with mean μ and covariance Σ . Consider two sequence of real numbers $\{a_P\}$ and $\{b_P\}$ indexed by P . Consider two sequences $\{a_P\}$ and $\{b_P\}$. The asymptotic notation $a_P = O(b_P)$ as $P \rightarrow \infty$ implies that there exists $K > 0, P_0$ such that for all $P \geq P_0$, we have $|a_P| \leq K|b_P|$. The asymptotic notation $a_P = o(b_P)$ means that for all $\epsilon > 0$, there exists $P_0(\epsilon) = P_0$ such that for all $P \geq P_0$, we have $|a_P| \leq \epsilon|b_P|$. We use $\log(\cdot)$ to denote the logarithm with base 2 and $\log_e(\cdot)$ to denote the natural logarithm. Define the thresholding operator $(\cdot)_+ = \max(\cdot, 0)$.

II. PROBLEM FORMULATION

We consider the point-to-point MIMO channel with a transmitter (Tx) and a legitimate receiver (Rx). There is a jammer (J) degrading the received signal at Rx and an eavesdropper (Eve) observing a noisy version of the transmitted signal. Define the channel matrices $\mathbf{H}_d \in \mathbb{C}^{n_r \times n_t}$ as the channel between Tx and Rx, $\mathbf{H}_e \in \mathbb{C}^{n_e \times n_t}$ as the channel between the Tx and Eve and $\mathbf{H}_j \in \mathbb{C}^{n_r \times n_j}$ as the channel between J and the Rx. The received signals at the legitimate receiver and Eve are respectively given by:

$$\mathbf{y} = \mathbf{H}_d \mathbf{x} + \mathbf{H}_j \mathbf{x}_j + \mathbf{n} \quad (\text{Rx}) \quad (1)$$

$$\bar{\mathbf{y}} = \mathbf{H}_e \mathbf{x} + \bar{\mathbf{n}} \quad (\text{Eve}) \quad (2)$$

where \mathbf{x} is the transmitted signal and \mathbf{x}_j is the jammer signal. The additive receiver noises \mathbf{n} and $\bar{\mathbf{n}}$ are assumed to be white and Gaussian distributed, i.e., $\mathbf{n} \sim \mathcal{N}_c(\mathbf{0}, \sigma^2 \mathbf{I}_{n_r})$, $\bar{\mathbf{n}} \sim \mathcal{N}_c(\mathbf{0}, \bar{\sigma}^2 \mathbf{I}_{n_e})$.

In this paper, we assume that Eve and J and cooperative in the sense that the jammer does not interfere with the eavesdropper signal. This can be realized in one of two ways. One way that this can be realized is if Eve and J are one simultaneous-transmit-and-receive unit, comprised of n_e receive antennas and n_j transmit antennas as depicted in Figure 1. Another way that this can be realized is to have Eve and J be separate nodes with Eve having $N_e = n_e + n_j$ receive antennas and J having n_j transmit antennas. Then, Eve can null out the undesired jammer interference by projecting its received signal in a subspace of dimension n_e , leading to the linear observation model (2). To illustrate this, say that Eve has N_e receive antennas and observes:

$$\mathbf{y}_e = \mathbf{G}_e \mathbf{x} + \mathbf{G}_j \mathbf{x}_j + \mathbf{n}_e$$

where \mathbf{G}_e is the channel from Tx to Eve, \mathbf{G}_j is the channel from J to Rx and \mathbf{n}_e is the receiver thermal noise at Eve. Considering the SVD of $\mathbf{G}_j = \mathbf{U}_j \Sigma_j \mathbf{V}_j^*$, we can choose $\mathbf{U}_{0,j} \in \mathbb{C}^{N_e \times n_e}$ to consist of the columns of \mathbf{U}_j corresponding to zero singular values. Then, defining the projection $\bar{\mathbf{y}} = \mathbf{U}_{0,j}^* \mathbf{y}_e$ ¹, we obtain the model (2) with $\mathbf{H}_e = \mathbf{U}_{0,j}^* \mathbf{G}_e$ and $\bar{\mathbf{n}} = \mathbf{U}_{0,j}^* \mathbf{n}_e$. Under the assumption that channel matrix elements are drawn i.i.d. from a continuous distribution, it follows that with probability 1, \mathbf{H}_e is full-rank and the equivalent model (2) can be used without loss of generality.

¹Here, $\text{Nul}(\mathbf{U}_{0,j}^*) = \text{Col}(\mathbf{G}_j)$ is the nullspace condition that is used in the nulling operation.

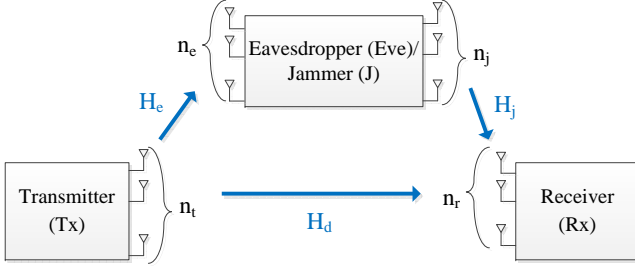


Fig. 1: Block diagram of secrecy communication problem in the presence of a jammer.

As in [11], [9], [10], we assume all elements of the channel matrices are drawn i.i.d. from a continuous distribution, and the channel values do not change during the signal transmission. The receiver is assumed to have perfect knowledge of \mathbf{H}_d and \mathbf{H}_j . As assumed in [11], [9], [10] we assume there is an error-free feedback link from the receiver to the transmitter. During the initial channel feedback phase, the receiver transmits its CSI using N_f bits due to limited bandwidth. Data transmission then follows where the transmitter designs its signal using quantized feedback.

A. Transmitter Strategy

Assuming $n_t > n_r$, the channel matrix \mathbf{H}_d has rank equal to n_r , which implies that there are $n_t - n_r$ dimensions available for artificial noise and n_r dimensions for information transmission.

We assume the transmitter splits its available power P into two components, the artificial noise and the information-bearing signal, using a linear combination:

$$\mathbf{x} = \sqrt{\rho}\mathbf{W}_1\mathbf{x}_s + \sqrt{1-\rho}\mathbf{W}_2\mathbf{x}_{an} \quad (3)$$

where $\mathbf{x}_s \in \mathbb{C}^{n_r}$ is the information bearing signal, $\mathbf{x}_{an} \in \mathbb{C}^{n_t-n_r}$ is artificial noise and ρ is the percentage of power allocated to \mathbf{x}_s . The linear precoding matrices $\mathbf{W}_1 \in \mathbb{C}^{n_t \times n_r}$ and $\mathbf{W}_2 \in \mathbb{C}^{n_t \times (n_t-n_r)}$ are assumed to be truncated unitary matrices. We also assume that \mathbf{x}_s is independent of \mathbf{x}_{an} . We let the covariance matrices of \mathbf{x}_s and \mathbf{x}_{an} be given by $\mathbf{K}_{x_s} \in \mathbb{C}^{n_r \times n_r}$ and $\mathbf{K}_{x_{an}} \in \mathbb{C}^{(n_t-n_r) \times (n_t-n_r)}$, respectively.

In order to design $(\mathbf{W}_1, \mathbf{W}_2)$ such that the artificial noise component cancels out at the receiver, the columns of \mathbf{W}_2 must lie in the null space of $\mathbf{H}_d \in \mathbb{C}^{n_r \times n_t}$. This can be accomplished through the singular value decomposition (SVD) of \mathbf{H}_d . Then, $\mathbf{H}_d\mathbf{W}_2 = \mathbf{0}$.

B. Receiver Strategy

The receiver has instantaneous knowledge of \mathbf{H}_d and \mathbf{H}_j . To null out the jammer's signal, the post-processing truncated unitary matrix $\mathbf{V} \in \mathbb{C}^{n_r \times (n_r-n_j)}$ at the receiver is applied:

$$\tilde{\mathbf{y}} = \mathbf{V}^*\mathbf{y} = \mathbf{V}^*\mathbf{H}_d\mathbf{x} + \tilde{\mathbf{n}} \quad (4)$$

where $\tilde{\mathbf{n}} = \mathbf{V}^*\mathbf{n} \sim \mathcal{N}_c(\mathbf{0}, \sigma^2\mathbf{I})$ since $\mathbf{V}^*\mathbf{V} = \mathbf{I}_{n_r-n_j}$. Consider the SVD of \mathbf{H}_j :

$$\begin{aligned} \mathbf{H}_j &= \mathbf{U}(\mathbf{H}_j)\mathbf{\Sigma}(\mathbf{H}_j)\mathbf{V}(\mathbf{H}_j)^* \\ &= [\mathbf{U}_1(\mathbf{H}_j)|\mathbf{U}_0(\mathbf{H}_j)] \begin{bmatrix} \mathbf{\Sigma}_1(\mathbf{H}_j) \\ \mathbf{0}_{n_r-n_j \times n_j} \end{bmatrix} \mathbf{V}(\mathbf{H}_j)^* \end{aligned}$$

Choosing the columns of \mathbf{V} span the left nullspace of \mathbf{H}_j , i.e.,

$$\mathbf{V} = \mathbf{U}_0(\mathbf{H}_j) \quad (5)$$

yields the desired nulling condition $\mathbf{V}^*\mathbf{H}_j = \mathbf{0}$.

C. Secrecy Degrees-of-Freedom (SDoF)

The secrecy capacity is known as a quantity measuring the maximal rate of reliable communication while maintaining secrecy to Eve [3]. The secrecy capacity is generally known to be [3], [5], [17]:

$$C_s = \max_{\mathbf{K}_{x_s} \succeq \mathbf{0}, \text{tr}(\mathbf{K}_{x_s}) \leq P} (I(\mathbf{x}_s; \tilde{\mathbf{y}}) - I(\mathbf{x}_s; \bar{\mathbf{y}}))_+$$

where $I(X; Y)$ denotes the mutual information between X and Y [18].

For a given input covariance matrix \mathbf{K}_{x_s} satisfying the power constraint $\text{tr}(\mathbf{K}_{x_s}) \leq P$, the achievable secrecy rate under the models (3) and (4) is given by:

$$R_s(\mathbf{K}_{x_s}) = (I(\mathbf{x}_s; \tilde{\mathbf{y}}) - I(\mathbf{x}_s; \bar{\mathbf{y}}))_+ \quad (6)$$

As Theorem 1 shows (see Appendix A), $R_s(\mathbf{K}_{x_s})$ will be positive for P large enough under certain assumptions, and thus the thresholding operator $(\cdot)_+$ can be omitted for the high SNR analysis to be presented in this paper. The (achievable) secure degrees-of-freedom (SDoF) are defined as:

$$d_s = \lim_{P \rightarrow \infty} \frac{R_s(\mathbf{K}_{x_s})}{\log P}$$

The intuitive meaning of this metric is that there are d_s data streams that can be reliably communicated to the receiver without having the eavesdropper being able to decode the transmitted information.

III. PERFECT CSI: ACHIEVABLE SECRECY RATE & SDOF

For the case of perfect CSI at the transmitter, the precoding matrix \mathbf{W}_2 can be designed as $\mathbf{W}_2 = \mathbf{V}_0(\mathbf{H}_d) \in \mathbb{C}^{n_t \times (n_t-n_r)}$, where the SVD of $\mathbf{H}_d \in \mathbb{C}^{n_r \times n_t}$ is given by

$$\begin{aligned} \mathbf{H}_d &= \mathbf{U}(\mathbf{H}_d)\mathbf{\Sigma}(\mathbf{H}_d)\mathbf{V}(\mathbf{H}_d)^* \\ &= \mathbf{U}(\mathbf{H}_d) [\mathbf{\Sigma}_1(\mathbf{H}_d)|\mathbf{0}_{n_r \times (n_t-n_r)}] [\mathbf{V}_1(\mathbf{H}_d)|\mathbf{V}_0(\mathbf{H}_d)]^* \end{aligned}$$

In that case, we can also choose $\mathbf{W}_1 = \mathbf{V}_1(\mathbf{H}_d) \in \mathbb{C}^{n_t \times n_r}$ in order to guarantee orthogonality between the information bearing signal $\mathbf{W}_1\mathbf{x}_s$ and the artificial noise signal $\mathbf{W}_2\mathbf{x}_{an}$. Then, the post-processed received signal at Rx and the received signal at Eve become:

$$\begin{aligned} \tilde{\mathbf{y}} &= \sqrt{\rho}\mathbf{V}^*\mathbf{H}_d\mathbf{W}_1\mathbf{x}_s + \tilde{\mathbf{n}} \\ &= \sqrt{\rho}\mathbf{V}^*\mathbf{U}(\mathbf{H}_d)\mathbf{\Sigma}_1(\mathbf{H}_d)\mathbf{V}_1(\mathbf{H}_d)^*\mathbf{V}_1(\mathbf{H}_d)\mathbf{x}_s + \tilde{\mathbf{n}} \\ &= \sqrt{\rho}\mathbf{V}^*\mathbf{U}(\mathbf{H}_d)\mathbf{\Sigma}_1(\mathbf{H}_d)\mathbf{x}_s + \tilde{\mathbf{n}} \\ &= \sqrt{\rho}\mathbf{H}\mathbf{x}_s + \tilde{\mathbf{n}} \\ \bar{\mathbf{y}} &= \sqrt{\rho}\mathbf{H}_e\mathbf{V}_1(\mathbf{H}_d)\mathbf{x}_s + \sqrt{1-\rho}\mathbf{H}_e\mathbf{V}_0(\mathbf{H}_d)\mathbf{x}_{an} + \bar{\mathbf{n}} \\ &= \sqrt{\rho}\mathbf{H}_{e,s}\mathbf{x}_s + \sqrt{1-\rho}\mathbf{H}_{e,an}\mathbf{x}_{an} + \bar{\mathbf{n}} \end{aligned}$$

where we defined $\mathbf{H} = \mathbf{V}^* \mathbf{U}(\mathbf{H}_d) \mathbf{\Sigma}_1(\mathbf{H}_d)$ as the transformed $(n_r - n_j) \times n_r$ channel matrix after post-processing. We also defined $\mathbf{H}_{e,s} = \mathbf{H}_e \mathbf{V}_1(\mathbf{H}_d)$ and $\mathbf{H}_{e,an} = \mathbf{H}_e \mathbf{V}_0(\mathbf{H}_d)$.

Using these expression for the received signals and the Gaussian noise assumptions, along with (6), we obtain an expression for the achievable secrecy rate under perfect CSI:

$$R_s(\mathbf{K}_{x_s}) = \log \det \left(\mathbf{I} + \frac{\rho}{\sigma^2} \mathbf{H} \mathbf{K}_{x_s} \mathbf{H}^* \right) - \log \left(\frac{\det(\rho \mathbf{H}_{e,s} \mathbf{K}_{x_s} \mathbf{H}_{e,s}^* + \frac{(1-\rho)P}{n_t - n_r} \mathbf{H}_{e,an} \mathbf{H}_{e,an}^* + \bar{\sigma}^2 \mathbf{I})}{\det(\frac{(1-\rho)P}{n_t - n_r} \mathbf{H}_{e,an} \mathbf{H}_{e,an}^* + \bar{\sigma}^2 \mathbf{I})} \right)$$

where we used $\mathbf{K}_{x_s} = \text{Cov}(\mathbf{x}_s)$ and $\mathbf{K}_{x_{an}} = \text{Cov}(\mathbf{x}_{an}) = \frac{P}{n_t - n_r} \mathbf{I}_{n_t - n_r}$.

The next theorem shows that $n_r - n_j$ SDoF are achievable under several mild assumptions.

Theorem 1. Assume the following:

- there exists constants $c_0, c_1 \in (0, 1/n_r]$ such that

$$c_0 P \mathbf{I} \preceq \mathbf{K}_{x_s} \preceq c_1 P \mathbf{I} \quad (7)$$

- $n_t > n_r > n_j$
- $n_e \leq n_t - n_r$

In the case of perfect CSI, it is possible to achieve up to $d_s = n_r - n_j$ SDoF at most.

Proof: See Appendix A. ■

We remark that the SDoF d_s is independent of n_e because the eavesdropper's rate $I(\mathbf{x}_s; \bar{\mathbf{y}})$ converges to a constant, dependent on n_e , and thus it has an asymptotically vanishing contribution to the SDoF, i.e., $\frac{I(\mathbf{x}_s; \bar{\mathbf{y}})}{\log P} \rightarrow 0$ as $P \rightarrow \infty$.

The achievable $d_s = n_r - n_j$ secure DoF is optimal since the jammer signal lies in a n_j -dimensional space and to null it out without any knowledge of its intrinsic dimension, receive beamforming leaves $n_r - n_j$ effective number of antennas at the receiver to use for successful decoding of the transmitted message.

The sufficient conditions of Thm. 1 are very mild, given our goal of achieving $n_r - n_j$ SDoF. If the condition $n_t > n_r$ is violated, the right nullspace of \mathbf{H}_d is empty, which implies that no precoding matrix \mathbf{W}_2 exists such that $\mathbf{H}_d \mathbf{W}_2 = \mathbf{0}$. If $n_r > n_j$ is violated, then no post-processing matrix \mathbf{V} exists such that $\mathbf{V}^* \mathbf{H}_j = \mathbf{0}$, i.e., the receiver does not have enough antennas to cancel the jammer's signal. If $n_e > n_t - n_r$, then the eavesdropper has enough antennas to recover at least one data stream containing information because the artificial noise signal spans at most a $(n_t - n_r)$ -dimensional space, leading to zero secrecy. The assumption $n_e + n_r \leq n_t$ was also made in Section VI in [14]. Thus, all assumptions are necessary to proceed.

IV. QUANTIZED CSI: ACHIEVABLE SECRECY RATE & SDoF

When there is imperfect CSI knowledge at the transmitter, the condition $\mathbf{H}_d \mathbf{W}_2 = \mathbf{0}$ will be violated and there will be some leakage of artificial noise at the receiver. As a consequence, the result of Theorem 1 no longer holds. In this section, we show that the same number of secure degrees-of-freedom can be achieved if the feedback rate scales fast enough as a function of transmit power.

A. Quantization on the Grassmann manifold

We assume that the receiver has perfect knowledge of the channel \mathbf{H}_d . Thus, it can perform the QR decomposition of the conjugate transpose of the channel matrix, i.e., \mathbf{H}_d^* :

$$\mathbf{H}_d^* = \mathbf{F} \mathbf{C} \quad (8)$$

where $\mathbf{C} \in \mathbb{C}^{n_r \times n_r}$ is an invertible matrix and $\mathbf{F} \in \mathbb{C}^{n_t \times n_r}$ is a tall orthonormal matrix whose columns span the same column space of \mathbf{H}_d^* . Thus, from the invertibility of \mathbf{C} , the condition $\mathbf{H}_d \mathbf{W}_2 = \mathbf{0}$ is equivalent to $\mathbf{F}^* \mathbf{W}_2 = \mathbf{0}$. A similar decomposition approach was considered in [10] for the MIMO interference channel. As in [10], a quantizer at the receiver uses N_f bits to describe the columns of \mathbf{F} and transmits the index of the quantized codeword back to the transmitter through a noiseless feedback link. The transmitter and receiver share a predefined codebook $\mathcal{S} = \{\mathbf{S}_1, \dots, \mathbf{S}_{2^{N_f}}\}$ consisting of truncated unitary matrices of size $n_t \times n_r$, which is designed using Grassmannian subspace packing. The quantization of the matrix \mathbf{F} on the Grassmann manifold \mathcal{G}_{n_t, n_r} is mathematically described by the minimum distance problem:

$$\hat{\mathbf{F}} = \arg \min_{\mathbf{S} \in \mathcal{S}} d_c(\mathbf{S}, \mathbf{F}) \quad (9)$$

where $d_c(\mathbf{S}, \mathbf{F}) = \frac{1}{\sqrt{2}} \|\mathbf{S} \mathbf{S}^* - \mathbf{F} \mathbf{F}^*\|_F$ is the chordal distance between \mathbf{S} and \mathbf{F} in \mathcal{G}_{n_t, n_r} .

B. Transmitter Strategy under Quantized CSI

Given the quantized matrix $\hat{\mathbf{F}} \in \mathbb{C}^{n_t \times n_r}$, the transmitter designs the linear precoding matrices $\mathbf{W}_{1,Q}$ and $\mathbf{W}_{2,Q}$. Let the matrix $\mathbf{W}_{2,Q} \in \mathbb{C}^{n_t \times n_t - n_r}$ be chosen such that

$$\hat{\mathbf{F}}^* \mathbf{W}_{2,Q} = \mathbf{0}_{n_r \times n_t - n_r} \quad (10)$$

This can be accomplished if the columns of $\mathbf{W}_{2,Q}$ are chosen to span the nullspace of $\hat{\mathbf{F}}^*$. We thus let $\mathbf{W}_{2,Q}$ be chosen such that its columns form a basis for $\text{Nul}(\hat{\mathbf{F}}^*)$.

In order to maximize the amount of information being sent over the noisy channel \mathbf{H}_d , the precoded information signal $\mathbf{W}_{1,Q} \mathbf{x}_s$ must always be orthogonal to the precoded artificial noise signal $\mathbf{W}_{2,Q} \mathbf{x}_{an}$. In order for this to hold irrespective of the signals \mathbf{x}_s and \mathbf{x}_{an} , $\mathbf{W}_{1,Q}$ must be orthogonal to $\mathbf{W}_{2,Q}$. This orthogonality implies that the matrix $\mathbf{W}_{1,Q} \in \mathbb{C}^{n_t \times n_r}$ must lie in the orthogonal complement of $\text{Nul}(\hat{\mathbf{F}}^*)$. In other words, we let the columns of $\mathbf{W}_{1,Q}$ form a basis for $\text{Col}(\hat{\mathbf{F}})$, i.e., $\mathbf{W}_{1,Q} = \hat{\mathbf{F}}$.

C. Receiver Strategy under Quantized CSI

Given \mathbf{y} , the receiver uses a post-processing matrix to form the transformed vector:

$$\tilde{\mathbf{y}} = \mathbf{G}^* \mathbf{V}^* \mathbf{y} \quad (11)$$

where \mathbf{V} is the nulling matrix for the jammer defined in (5) and \mathbf{y} is the received signal in (1). Given that \mathbf{V} is already chosen using (5), we want to design $\mathbf{G} \in \mathbb{C}^{d_s \times d_s}$ as a function of $\mathbf{V}, \mathbf{F}, \mathbf{C}$ (all of which are available at the receiver). Let us choose \mathbf{G} as:

$$\mathbf{G}^* = \mathbf{B}^* \mathbf{F} \mathbf{C} \mathbf{V} (\mathbf{V}^* \mathbf{C}^* \mathbf{C} \mathbf{V})^{-1} \quad (12)$$

where $\mathbf{B} \in \mathbb{C}^{n_t \times d_s}$ is a tall truncated unitary matrix of full rank.

Let the leakage term be given by

$$\mathbf{e}_L = \sqrt{1 - \rho} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{x}_{an}$$

The post-processed received signal can be written as

$$\begin{aligned} \tilde{\mathbf{y}} &= \mathbf{G}^* (\mathbf{V}^* \mathbf{H}_d \mathbf{x} + \tilde{\mathbf{n}}) \\ &= \sqrt{\rho} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{1,Q} \mathbf{x}_s + \mathbf{e}_L + \mathbf{G}^* \tilde{\mathbf{n}} \end{aligned}$$

D. Controlling the Leakage Power

The next lemma bounds the power of the leakage term.

Lemma 1. *Assuming a quantization codebook construction based on sphere-packing using N_f bits, the leakage power is bounded as:*

$$L(P) := \mathbb{E} \|\mathbf{e}_L\|_2^2 \leq \frac{2(1 - \rho)P}{n_t - n_r} \left(\frac{2}{(c2^{N_f})^{1/N}} \right)^2 (1 + o(2^{-N_f/N})) \quad (13)$$

where $N = 2n_r(n_t - n_r)$ and c is a constant.

Proof: See Appendix B. ■

The corollary that follows provides a sufficient condition on the feedback rate to ensure that the leakage power stays bounded. This will be a key condition that will be used to prove the optimal SDoF scaling.

Corollary 1. *Assume that the quantization with N_f feedback bits scales as:*

$$N_f = \frac{N}{2} \log_2 P = n_r(n_t - n_r) \log_2 P \quad (14)$$

Then, the leakage power $L(P)$ stays bounded as $P \rightarrow \infty$, i.e., $L(P) = O(1)$ as $P \rightarrow \infty$.

Proof: See Appendix C. ■

We note that boundedness of the leakage power does not necessarily imply the achievability of the optimal SDoF. However, it provides a grasp on the feedback bit rate scaling that can possibly guarantee such a claim. Next, we show that the scaling condition (14) is sufficient to guarantee the optimal SDoF gain.

E. SDoF Analysis

Here, we show that the secrecy rate of the quantized CSI scheme achieves the same SDoF as the corresponding scheme with perfect CSI as derived in Theorem 1. In other words, there is no performance loss for large enough SNR.

Under the transmitter and receiver strategies proposed for quantized CSI, the achievable secrecy rate when CSI is perfect is given in (15) by:

$$R_{s,G}^P = R_{s,G}^P(\mathbf{K}_{x_s}) = I(\mathbf{x}_s; \tilde{\mathbf{y}}) - I(\mathbf{x}_s; \bar{\mathbf{y}}),$$

where the subscript s denotes secrecy and the subscript G denotes post-processing with the matrix \mathbf{G}^* in addition to \mathbf{V}^* (recall (11)). Similarly, when only quantized CSI is available, the achievable secrecy rate is given by $R_{s,G}^Q$ in (16), where $(\mathbf{W}_{1,Q}, \mathbf{W}_{2,Q})$ are the designed precoding matrices under

imperfect CSI. We note that in general $\mathbf{W}_1 \neq \mathbf{W}_{1,Q}$ and $\mathbf{W}_2 \neq \mathbf{W}_{2,Q}$, although they have the same rank.

Before proving the main result, we will need a few technical lemmas. We first recall the variational representation of the log-determinant function.

Lemma 2. [19] *Let $\mathbf{E} \in \mathbb{C}^{n \times n}$ be a positive definite matrix. Then,*

$$\log_e \det(\mathbf{E}^{-1}) = \max_{\mathbf{S} \succeq \mathbf{0}} \{-\text{tr}(\mathbf{S}\mathbf{E}) + \log_e \det(\mathbf{S}) + n\}$$

and the optimal solution is $\mathbf{S}^ = \mathbf{E}^{-1}$.*

Lemma 2 implies the following perturbation bounds, which will be crucial for analyzing the secrecy rate performance.

Lemma 3. *Let \mathbf{A} and $\mathbf{A} + \mathbf{\Delta}$ be positive definite matrices. Then, the following bounds hold:*

$$\begin{aligned} \log_e \det(\mathbf{A} + \mathbf{\Delta}) - \log_e \det(\mathbf{A}) &\leq \text{tr}(\mathbf{A}^{-1} \mathbf{\Delta}) \\ \log_e \det(\mathbf{A} + \mathbf{\Delta}) - \log_e \det(\mathbf{A}) &\geq \text{tr}(\mathbf{\Delta}(\mathbf{A} + \mathbf{\Delta})^{-1}) \end{aligned}$$

We will need a technical lemma that yields an asymptotic lower bound to a remainder term that will be crucial for proving the main result of the paper (Theorem 2).

Lemma 4. *Consider the transmitter and receiver strategies described in Section IV. Assume the same conditions as in Theorem 1. In addition, assume (14). Define the auxiliary variable $\beta(P)$ as:*

$$\begin{aligned} \beta(P) &= \log \det \left(\rho P \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{1,Q} \mathbf{W}_{1,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} \right. \\ &\quad \left. + (1 - \rho) \frac{P}{n_t - n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G} \right) \\ &\quad - \log \det \left(\rho P \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{1,Q} \mathbf{W}_{1,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G} \right) \end{aligned}$$

Then, there exists a non-negative sequence $\{\epsilon(P)\}$ converging to zero such that for all P :

$$\beta(P) \geq -\epsilon(P)$$

Proof: See Appendix D. ■

The main result of the paper is provided in Theorem 2, where the optimal SDoF is shown to be obtained under the quantized feedback of CSI. In addition, it is shown that there is no secrecy rate loss due to quantization asymptotically as $P \rightarrow \infty$.

Theorem 2. *Consider the transmitter and receiver strategies described in Section IV. Assume the same conditions as in Theorem 1.*

1) *Assuming (14), i.e.,*

$$N_f = \frac{N}{2} \log_2 P$$

then, the full $d_s^Q = d_s = n_r - n_j$ SDoF are achievable.

2) *Assuming for some $\epsilon > 0$,*

$$N_f = (1 + \epsilon) \frac{N}{2} \log_2 P \quad (17)$$

then, the full $d_s^Q = d_s = n_r - n_j$ SDoF are achievable and the asymptotic rate gap due to quantization $\delta_{GAP} := \lim_{P \rightarrow \infty} \{R_{s,G}^P - R_{s,G}^Q\}$ is zero.

$$R_{s,G}^P = \underbrace{\log \left(\frac{\det(\rho \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_1 \mathbf{K}_{x_s} \mathbf{W}_1^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G})}{\det(\sigma^2 \mathbf{G}^* \mathbf{G})} \right)}_{T_+^P} - \underbrace{\log \left(\frac{\det(\rho \mathbf{H}_e \mathbf{W}_1 \mathbf{K}_{x_s} \mathbf{W}_1^* \mathbf{H}_e^* + \frac{(1-\rho)P}{n_t-n_r} \mathbf{H}_e \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_e^* + \bar{\sigma}^2 \mathbf{I}_{n_e})}{\det(\frac{(1-\rho)P}{n_t-n_r} \mathbf{H}_e \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_e^* + \bar{\sigma}^2 \mathbf{I}_{n_e})} \right)}_{T_-^P} \quad (15)$$

$$R_{s,G}^Q = \underbrace{\log \left(\frac{\det(\rho \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{1,Q} \mathbf{K}_{x_s} \mathbf{W}_{1,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \frac{(1-\rho)P}{n_t-n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G})}{\det(\frac{(1-\rho)P}{n_t-n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G})} \right)}_{T_+^Q} - \underbrace{\log \left(\frac{\det(\rho \mathbf{H}_e \mathbf{W}_{1,Q} \mathbf{K}_{x_s} \mathbf{W}_{1,Q}^* \mathbf{H}_e^* + \frac{(1-\rho)P}{n_t-n_r} \mathbf{H}_e \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_e^* + \bar{\sigma}^2 \mathbf{I}_{n_e})}{\det(\frac{(1-\rho)P}{n_t-n_r} \mathbf{H}_e \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_e^* + \bar{\sigma}^2 \mathbf{I}_{n_e})} \right)}_{T_-^Q} \quad (16)$$

Proof: See Appendix E. ■

Remark 1. The scaling condition (17) can be weakened to

$$N_f = \frac{N}{2} \log_2(Pm(P))$$

where $m(P)$ is any nonnegative function satisfying $m(P) \rightarrow \infty$ as $P \rightarrow \infty$.

We finally remark that having N_f be a monotonically increasing function in P is not enough to guarantee $\delta_{\text{GAP}} = 0$. This can be seen from the proof of Theorem 2, where in order for δ_{GAP} to converge to zero as $P \rightarrow \infty$, we need the following condition to hold:

$$\mathbf{U}(P) = P \cdot \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} \rightarrow \mathbf{0}$$

which implies that $\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} = o(P^{-1})$. The condition $N_f \rightarrow \infty$ alone only implies $\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} = o(1)$ and does not guarantee $\mathbf{U}(P) \rightarrow \mathbf{0}$. Necessary conditions that guarantee the results of Theorem 2 remain an open problem.

V. SIMULATIONS

This section contains a few illustrative simulations that validate the methodology presented throughout the paper. The elements of all channels were generated as i.i.d. random complex-normal $\mathcal{N}_c(0, 1)$ random variables as in [9], [10].

Figure 2 shows the secrecy rate performance as a function of transmit SNR for $n_r = 2, 3, 4$ where $n_j = 1$ and $n_t = 2n_r, n_e = n_t - n_r = n_r$. The feedback bit rate increases as a function of P according to (14) for the left panel and according to (17) for the right panel. The secrecy rate for the perfect CSI and quantized CSI schemes were calculated using the expressions in (15) and (16) with the choices $\mathbf{K}_{x_s} = \frac{P}{n_r} \mathbf{I}_{n_r}$ and $\mathbf{K}_{x_a n} = \frac{P}{n_t - n_r} \mathbf{I}_{n_t - n_r}$. Due to the high complexity associated with implementing (9) for large bit rates N_f , we adopt the random perturbation scheme of [10] to generate the quantized matrices $\hat{\mathbf{F}}^2$. It was shown numerically

in [10] that this approximation is fairly accurate for a wide range of SNR. It is evident from Figure 2 that the slopes of the secrecy rate curves become identical as SNR grows, implying that the SDoF become identical, as expected from Theorem 2. In addition, for $N_f = \frac{(1+\epsilon)N}{2} \log_2 P$ with $\epsilon = 0.5$, the right panel of Figure 2 shows that the secrecy rate gap converges to zero as P grows to infinity.

Figure 3 shows the secrecy rate performance as a function of SNR for $n_r = 3$ where $n_t = 2n_r$ and $n_e = n_t - n_r$. The feedback bit rate is fixed to $N_f = 30, 60, 90$ and it is observed that the secrecy rate converges to a limiting value as the transmit SNR grows to infinity. Similar behavior is observed for the communication rate performance with finite rate feedback without secrecy or jamming in [9], [10], [7], [8] and without jamming in [14]. This phenomenon is due to the fact that finite quantization bit rate allows the artificial noise to dominate at the receiver and as a result, the secure multiplexing gain becomes zero.

Figure 4 shows the loss in secrecy rate due to quantization, for fixed SNR and number of antennas, as a function of number of feedback bits N_f . The SNR is fixed to $\text{SNR} = 10, 20, 30$ dB and we observe that the secrecy rate loss converges to zero fast as N_f grows. We conjecture that this rate gap converges to zero exponentially fast as a function of N_f .

VI. CONCLUSION

We studied the value of quantized feedback for MIMO secrecy communications in the presence of a jammer. We proposed transmitter and receiver strategies based on linear precoding and receive beamforming to simultaneously combat jammer interference, imperfect CSI at the transmitter and eavesdropping. Under this MIMO communication model, we characterized the achievable secrecy rate performance of the system. We derived sufficient conditions on the feedback bit rate scaling as a function of transmit power that guarantees the same secure degrees-of-freedom as the corresponding scheme with perfect CSI. We also showed that there is no secrecy rate loss due to quantization asymptotically as $P \rightarrow \infty$ under

²The reason why $n_t \geq 2n_r$ is chosen here has to do with the approximation of the quantization. While not pursued in this paper, the case $n_t < 2n_r$ can be covered in a similar manner. For more details, see Section VI.B in [10].

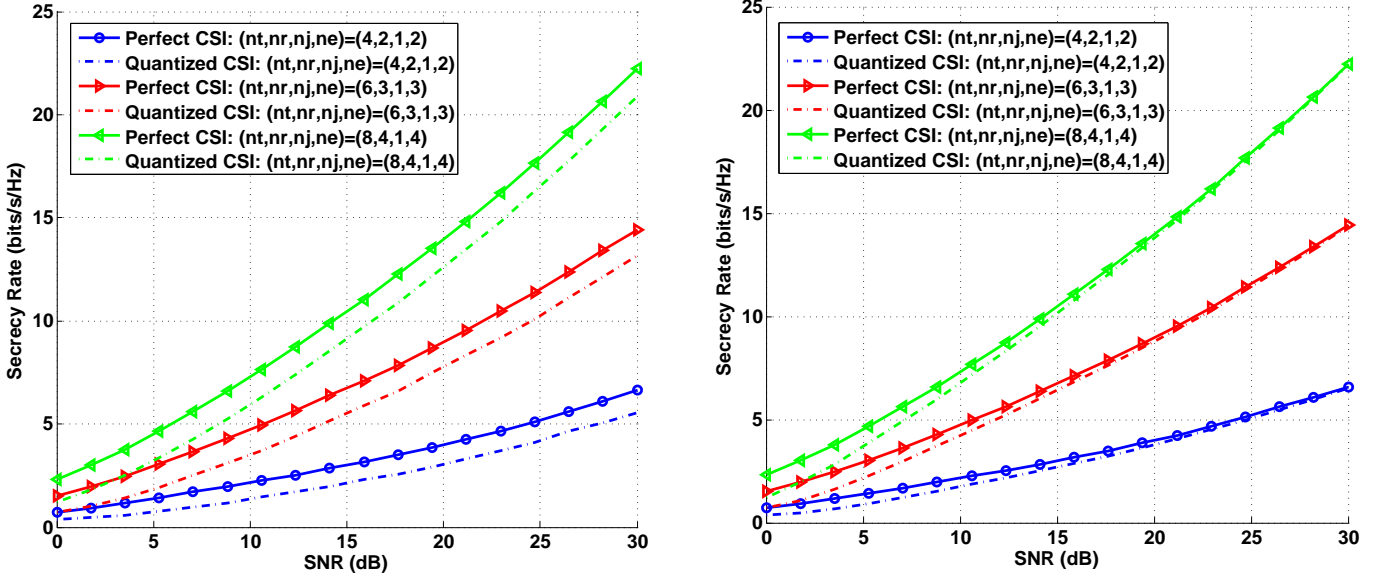


Fig. 2: Monte Carlo simulation for secrecy rate performance as a function of SNR for $N_f = \frac{N}{2} \log_2 P$ (left panel) and $N_f = \frac{(1+0.5)N}{2} \log_2 P$ (right panel). The transmitter has $n_t = 2n_r$ antennas and the receiver has $n_r = 2, 3, 4$ antennas. The jammer is equipped with one antenna, i.e., $n_j = 1$, and the eavesdropper is equipped with $n_e = n_t - n_r = n_r$ antennas. Equal power allocation $\rho = 1/2$ was used. For high SNR, the slope of the secrecy rate curves corresponding to quantized CSI become identical to the slope of the curves with perfect CSI, as predicted by Theorem 2. The corresponding slopes are $d_s = 1, 2, 3$. As predicted in Theorem 2, the secrecy rate gap converges to zero as $P \rightarrow \infty$ since N_f increases slightly faster than prescribed in (14) (see right panel).

the same conditions. Simulations were shown to validate the theoretical analysis.

Future work may include deriving necessary conditions on the feedback bit rate to maintain the optimal secure degrees-of-freedom and developing efficient power allocations algorithms to improve performance in the low SNR regime. Another worthwhile open problem is to bound the secrecy rate gap as a function of finite power P and number of feedback bits N_f . This type of analysis would provide insight into how many feedback bits are needed to achieve an arbitrarily small secrecy rate gap.

ACKNOWLEDGMENT

The author gratefully acknowledges discussions with David Browne and Keith W. Forsythe.

APPENDIX A PROOF OF THEOREM 1

Proof: Decompose R_s into two components $R_s = R_s^d - R_s^E$ where

$$R_s^d = \log \det \left(\mathbf{I} + \frac{\rho}{\sigma^2} \mathbf{H} \mathbf{K}_{x_s} \mathbf{H}^* \right)$$

$$R_s^E = \log \left(\frac{\det(\rho \mathbf{H}_{e,s} \mathbf{K}_{x_s} \mathbf{H}_{e,s}^* + \frac{(1-\rho)P}{n_t - n_r} \mathbf{H}_{e,an} \mathbf{H}_{e,an}^* + \bar{\sigma}^2 \mathbf{I})}{\det(\frac{(1-\rho)P}{n_t - n_r} \mathbf{H}_{e,an} \mathbf{H}_{e,an}^* + \bar{\sigma}^2 \mathbf{I})} \right)$$

Expanding R_s^d , we obtain:

$$R_s^d = \sum_{i=1}^{n_r - n_j} \log \left(1 + \frac{\rho}{\sigma^2} \lambda_i(\mathbf{H} \mathbf{K}_{x_s} \mathbf{H}^*) \right)$$

$$= d_s \log(P) + \sum_{i=1}^{d_s} \log \left(P^{-1} + \frac{\rho}{\sigma^2} \frac{\lambda_i(\mathbf{H} \mathbf{K}_{x_s} \mathbf{H}^*)}{P} \right) \quad (18)$$

Using (7), it is guaranteed that all eigenvalues $\lambda_i(\mathbf{H} \mathbf{K}_{x_s} \mathbf{H}^*)$ satisfy the bounds:

$$c_0 P \lambda_i(\mathbf{H} \mathbf{H}^*) \leq \lambda_i(\mathbf{H} \mathbf{K}_{x_s} \mathbf{H}^*) \leq c_1 P \lambda_i(\mathbf{H} \mathbf{H}^*) \quad (19)$$

Since the matrix $\mathbf{H} \mathbf{H}^*$ is positive definite almost surely, using (19) into (18) and taking the limit as $P \rightarrow \infty$, we obtain $\frac{R_s^d}{\log(P)} \xrightarrow{P \rightarrow \infty} d_s$. To finish the proof, it remains to show $\frac{R_s^E}{\log(P)} \xrightarrow{P \rightarrow \infty} 0$. To prove this, note that R_s^E converges to a constant as $P \rightarrow \infty$:

$$R_s^E = \log \det \left(\mathbf{I} + \rho \mathbf{H}_{e,s} \mathbf{K}_{x_s} \mathbf{H}_{e,s}^* \left(\frac{(1-\rho)P \mathbf{H}_{e,an} \mathbf{H}_{e,an}^*}{n_t - n_r} + \bar{\sigma}^2 \mathbf{I} \right)^{-1} \right)$$

$$\leq \log \det \left(\mathbf{I} + c_1 \rho P \mathbf{H}_{e,s} \mathbf{H}_{e,s}^* \left(\frac{(1-\rho)P \mathbf{H}_{e,an} \mathbf{H}_{e,an}^*}{n_t - n_r} + \bar{\sigma}^2 \mathbf{I} \right)^{-1} \right)$$

$$= \log \det \left(\mathbf{I} + c_1 \rho \mathbf{H}_{e,s} \mathbf{H}_{e,s}^* \left(\frac{(1-\rho) \mathbf{H}_{e,an} \mathbf{H}_{e,an}^*}{n_t - n_r} + \bar{\sigma}^2 P^{-1} \mathbf{I} \right)^{-1} \right)$$

$$\xrightarrow{P \rightarrow \infty} \log \det \left(\mathbf{I} + c_1 \frac{\rho(n_t - n_r)}{1 - \rho} \mathbf{H}_{e,s} \mathbf{H}_{e,s}^* (\mathbf{H}_{e,an} \mathbf{H}_{e,an}^*)^{-1} \right)$$

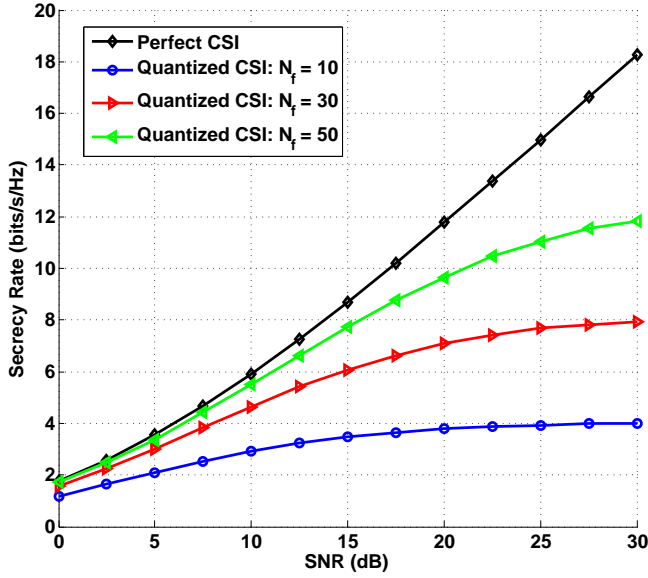


Fig. 3: Monte Carlo simulation for secrecy rate loss due to quantization as a function of SNR for $N_f = 30, 60, 90$. The transmitter has $n_t = 2n_r$ antennas and the receiver has $n_r = 3$ antennas. The eavesdropper has $n_e = n_t - n_r = 3$ antennas and the eavesdropper has a single antenna. Equal power allocation $\rho = 1/2$ was used. The secrecy rate saturates to a limiting value as SNR grows, implying zero SDoF gain.

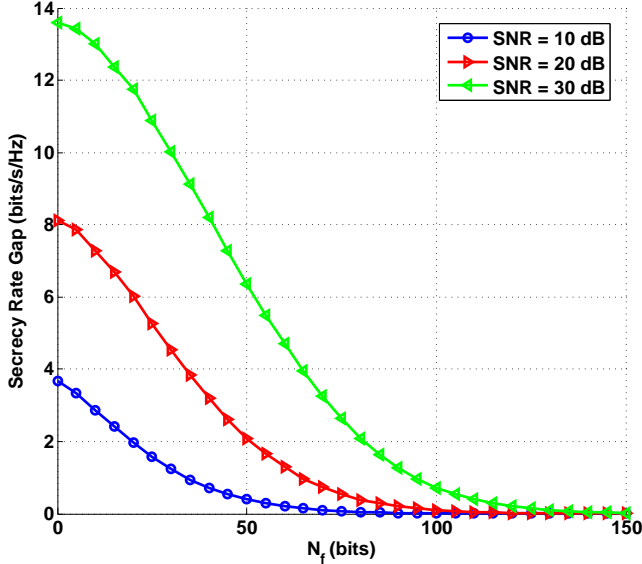


Fig. 4: Monte Carlo simulation for secrecy rate loss due to quantization as a function of N_f for fixed SNR . The transmitter has $n_t = 2n_r$ antennas and the receiver has $n_r = 3$ antennas. The jammer has $n_j = 1$ antenna and the eavesdropper has $n_e = n_t - n_r = 3$ antennas. Equal power allocation $\rho = 1/2$ was used. The secrecy rate gap converges to zero fast as the number of feedback bits increase.

Note that we used the fact that $n_e \leq n_t - n_r$, implying that $\mathbf{H}_{e,an} \mathbf{H}_{e,an}^*$ is full rank. Using a similar argument and (7) again, it follows that R_s^E is bounded below by a constant as $P \rightarrow \infty$ as well. Thus, $R_s^E / \log(P) \rightarrow 0$ and the proof is complete. ■

APPENDIX B PROOF OF LEMMA 1

Proof: The transmitter has access to $\hat{\mathbf{F}}$, a quantized version of \mathbf{F} , which is obtained using (9). The transmitter designs $\mathbf{W}_{2,Q}$ such that $\hat{\mathbf{F}}^* \mathbf{W}_{2,Q} = 0$ (recall (10)). Letting $\hat{\mathbf{M}} = \hat{\mathbf{F}}\mathbf{U}$, we also have $\hat{\mathbf{M}}^* \mathbf{W}_{2,Q} = 0$. Using this, we obtain:

$$\begin{aligned} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} &= \mathbf{G}^* \mathbf{V}^* \mathbf{C}^* \mathbf{F}^* \mathbf{W}_{2,Q} \\ &= \mathbf{B}^* \mathbf{F} \mathbf{C} \mathbf{V} (\mathbf{V}^* \mathbf{C}^* \mathbf{C} \mathbf{V})^{-1} (\mathbf{C} \mathbf{V})^* \mathbf{F}^* \mathbf{W}_{2,Q} \end{aligned}$$

Consider the square invertible positive definite matrix

$$\mathbf{P} = \mathbf{C} \mathbf{V} (\mathbf{V}^* \mathbf{C}^* \mathbf{C} \mathbf{V})^{-1} (\mathbf{C} \mathbf{V})^* \quad (20)$$

This matrix can be seen as a projection onto the column space of $\mathbf{C} \mathbf{V}$. Write the eigendecomposition of \mathbf{P} as $\mathbf{U} \mathbf{\Lambda} \mathbf{U}^*$. Then, continuing:

$$\begin{aligned} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} &= \mathbf{B}^* \mathbf{F} \mathbf{P} \mathbf{F}^* \mathbf{W}_{2,Q} \\ &= \mathbf{B}^* \mathbf{F} \mathbf{U} \mathbf{\Lambda} \mathbf{U}^* \mathbf{F}^* \mathbf{W}_{2,Q} \\ &= \mathbf{B}^* \mathbf{M} \mathbf{\Lambda} \mathbf{M}^* \mathbf{W}_{2,Q} \\ &= \mathbf{B}^* \mathbf{M} \mathbf{\Lambda} \mathbf{M}^* \mathbf{W}_{2,Q} - \mathbf{B}^* \hat{\mathbf{M}} \hat{\mathbf{M}}^* \mathbf{W}_{2,Q} \\ &= \mathbf{B}^* (\mathbf{M} \mathbf{\Lambda} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*) \mathbf{W}_{2,Q} \end{aligned}$$

The leakage power can then be bounded as:

$$\begin{aligned} L &= \mathbb{E} \|\sqrt{1-\rho} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{x}_{an}\|_2^2 \\ &\leq (1-\rho) \mathbb{E} \|\mathbf{x}_{an}\|_2^2 \|\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q}\|_F^2 \\ &= \frac{(1-\rho)P}{n_t - n_r} \|\mathbf{B}^* (\mathbf{M} \mathbf{\Lambda} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*) \mathbf{W}_{2,Q}\|_F^2 \\ &\leq \frac{(1-\rho)P}{n_t - n_r} \|\mathbf{B}^*\|_2^2 \|\mathbf{M} \mathbf{\Lambda} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*\|_F^2 \|\mathbf{W}_{2,Q}\|_2^2 \\ &= \frac{(1-\rho)P}{n_t - n_r} \|\mathbf{M} \mathbf{\Lambda} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*\|_F^2 \end{aligned} \quad (21)$$

where we used the fact that $\|\mathbf{B}^*\|_2 = \|\mathbf{W}_{2,Q}\|_2 = 1$ since they are truncated unitary matrices.

Since \mathbf{P} is a projection matrix, it follows its eigenvalues $[\mathbf{\Lambda}]_{i,i}$ are either 1 or 0. As a result, we have:

$$\|\mathbf{M} \mathbf{\Lambda} \mathbf{M}^*\|_F^2 \leq \|\mathbf{M} \mathbf{M}^*\|_F^2 \quad (23)$$

and since $\mathbf{I} - \mathbf{\Lambda} =: \mathbf{D}$ consists of zeros or ones on the diagonal, we also have:

$$\begin{aligned} \text{tr}(\hat{\mathbf{M}}^* \mathbf{M} (\mathbf{I} - \mathbf{\Lambda}) (\hat{\mathbf{M}}^* \mathbf{M})^*) &= \text{tr}(\tilde{\mathbf{M}} \mathbf{D} \tilde{\mathbf{M}}^*) = \text{tr}(\mathbf{D} \tilde{\mathbf{M}}^* \tilde{\mathbf{M}}) \\ &= \sum_i [\mathbf{D}]_{i,i} [\tilde{\mathbf{M}}^* \tilde{\mathbf{M}}]_{i,i} \geq 0 \end{aligned} \quad (24)$$

Using (23) and (24), we obtain:

$$\|\mathbf{M} \mathbf{\Lambda} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*\|_F^2 \leq \|\mathbf{M} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*\|_F^2 \quad (25)$$

Using the bound (25) in (22), we obtain:

$$\begin{aligned} L &\leq \frac{(1-\rho)P}{n_t - n_r} \|\mathbf{M} \mathbf{M}^* - \hat{\mathbf{M}} \hat{\mathbf{M}}^*\|_F^2 \\ &= \frac{(1-\rho)P}{n_t - n_r} \|\mathbf{F} \mathbf{F}^* - \hat{\mathbf{F}} \hat{\mathbf{F}}^*\|_F^2 \\ &= \frac{2(1-\rho)P}{n_t - n_r} d_c(\mathbf{F}, \hat{\mathbf{F}})^2 \end{aligned} \quad (26)$$

where we used $\mathbf{U}\mathbf{U}^* = \mathbf{I}_{n_r}$ and the definition of the chordal distance.

Assuming a sphere-packing codebook construction, Thm. 5 in [20] yields a bound on the maximum quantization error:

$$\max_{\mathbf{F} \in \mathcal{G}_{n_t, n_r}} d_c(\mathbf{F}, \hat{\mathbf{F}}) \leq \frac{2}{(c2^{N_f})^{1/N}} (1 + o(2^{-\frac{N_f}{N}})) \quad (27)$$

where $\hat{\mathbf{F}}$ is obtained using (9) and c is the coefficient of the ball volume in \mathcal{G}_{n_t, n_r} ³. Using the quantization error bound (27) in (26), we obtain the desired bound in (13). ■

APPENDIX C PROOF OF COROLLARY 1

Proof: With the choice $N_f = N/2 \log_2 P$, Lemma 1 implies

$$L \leq \frac{2(1-\rho)P}{n_t - n_r} \frac{4/c^2}{P} (1 + o(P^{-1/2}))$$

$$\xrightarrow{P \rightarrow \infty} \frac{8(1-\rho)/c^2}{n_t - n_r}$$

The proof is complete. ■

APPENDIX D PROOF OF LEMMA 4

Proof: We want to show that $\beta(P)$ is positive asymptotically as $P \rightarrow \infty$. Define the matrices

$$\begin{aligned} \mathbf{M}_1(P) &= \rho P \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_1 \mathbf{W}_1^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} \\ \mathbf{M}_2(P) &= (1-\rho) \frac{P}{n_t - n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} \\ \mathbf{A}(P) &= \mathbf{M}_1(P) + \mathbf{M}_2(P) + \sigma^2 \mathbf{G}^* \mathbf{G} \\ \mathbf{\Gamma}(P) &= \mathbf{W}_{1,Q} \mathbf{W}_{1,Q}^* - \mathbf{W}_1 \mathbf{W}_1^* \\ \mathbf{Z} &= \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \end{aligned}$$

and the scalar $\delta = \rho P$. Then, we can write:

$$\beta(P) = \log \det(\mathbf{A}(P) + \delta(P) \mathbf{Z} \mathbf{\Gamma}(P) \mathbf{Z}^*) - \log \det(\mathbf{A}(P)).$$

Recall the choice $\mathbf{W}_{1,Q} = \hat{\mathbf{F}}$ and $\mathbf{W}_1 = \mathbf{F}$. Thus, the matrix $\mathbf{\Gamma}(P)$ can be rewritten as:

$$\mathbf{\Gamma}(P) = \hat{\mathbf{F}} \hat{\mathbf{F}}^* - \mathbf{F} \mathbf{F}^*$$

If $\hat{\mathbf{F}} \hat{\mathbf{F}}^* \succeq \mathbf{F} \mathbf{F}^*$, then it follows that $\beta(P) \geq 0$ for all P , but there is not necessarily true in general. Instead, we show $\beta(P) \geq 0$ for large P . Using the perturbation Lemma 3 with $\Delta(P) = \delta(P) \mathbf{Z} \mathbf{\Gamma}(P) \mathbf{Z}^*$, we obtain

$$\begin{aligned} \beta(P) &\geq \text{tr}(\Delta(P)(\mathbf{A}(P) + \Delta(P))^{-1}) \log(e) \\ &\geq -\|\Delta(P)\|_F \|(\mathbf{A}(P) + \Delta(P))^{-1}\|_F \log(e) \end{aligned} \quad (28)$$

³The constant c is given by [21]:

$$c = \frac{1}{(n_r(n_t - n_r))!} \prod_{i=1}^{n_r} \frac{(n_t - i)!}{(n_r - i)!}$$

We conclude the proof by showing that $\|\Delta(P)\|_F \cdot \|(\mathbf{A}(P) + \Delta(P))^{-1}\|_F = o(1)$ as $P \rightarrow \infty$. To this end, first note the bounds:

$$\begin{aligned} \|\Delta(P)\|_F &= \delta(P) \|\mathbf{Z} \mathbf{\Gamma}(P) \mathbf{Z}^*\|_F \\ &\leq \delta(P) \|\mathbf{Z}\|_2^2 \|\mathbf{\Gamma}(P)\|_F \\ &= \sqrt{2} \rho P \|\mathbf{Z}\|_2^2 d_c(\mathbf{F}, \hat{\mathbf{F}}) \\ &\leq \sqrt{2} P \frac{2 \|\mathbf{Z}\|_2^2 2^{-N_f/N}}{c^{1/N}} (1 + o(2^{-N_f/N})) \Bigg|_{N_f = \frac{N}{2} \log_2 P} \\ &= O(\sqrt{P}) \quad (\text{as } P \rightarrow \infty) \end{aligned} \quad (29)$$

where we used the upper bound (27) on the chordal distance in (29). Next, consider the positive semidefinite matrix $\mathbf{M}_2(P)$. Using the bounds in the proof of Lemma 1 (see (21)), it follows that:

$$\begin{aligned} \text{tr}(\mathbf{M}_2(P)) &= \frac{(1-\rho)P}{n_t - n_r} \text{tr}(\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G}) \\ &= \frac{(1-\rho)P}{n_t - n_r} \|\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q}\|_F^2 \\ &\leq \frac{2(1-\rho)P}{n_t - n_r} d_c(\mathbf{F}, \hat{\mathbf{F}})^2 \\ &\leq \frac{4(1-\rho)P}{c^{2/N} (n_t - n_r)} 2^{-2N_f/N} (1 + o(2^{-N_f/N})) \Bigg|_{N_f = \frac{N}{2} \log_2 P} \\ &\leq \frac{4(1-\rho)}{c^{2/N} (n_t - n_r)} (1 + o(P^{-1/2})) \\ &= O(1) \quad (\text{as } P \rightarrow \infty) \end{aligned} \quad (31)$$

On the other hand, the sequence of matrices $\mathbf{M}_1(P)$ converges to infinity as $P \rightarrow \infty$ since $\mathbf{M}_1(P) = \rho P \mathbf{K}_{\text{const}}$ for some constant strictly positive definite matrix $\mathbf{K}_{\text{const}}$ ⁴. Thus, we have:

$$\begin{aligned} \|(\mathbf{A}(P) + \Delta(P))^{-1}\|_F &= \|(\rho P \mathbf{K}_{\text{const}} + \mathbf{M}_2(P) + \sigma^2 \mathbf{G}^* \mathbf{G} + \Delta(P))^{-1}\|_F \\ &= P^{-1} \left\| \left(\rho \mathbf{K}_{\text{const}} + \left\{ \frac{\mathbf{M}_2(P) + \sigma^2 \mathbf{G}^* \mathbf{G} + \Delta(P)}{P} \right\} \right)^{-1} \right\|_F \end{aligned} \quad (32)$$

Next, we notice that the term in the brackets above is $O(P^{-1/2})$ since \mathbf{G} is independent of P and from (31) and (30):

$$\begin{aligned} \text{tr} \left(\frac{\mathbf{M}_2(P)}{P} \right) &= O(P^{-1}) \\ \left\| \frac{\Delta(P)}{P} \right\|_F &= O(P^{-1/2}) \end{aligned}$$

Since the trace of the sequence of positive semidefinite matrices $\{\mathbf{M}_2(P)\}$ tends to zero, the sequence of the matrices must

⁴In fact, the matrix $\mathbf{K}_{\text{const}}$ can be shown to be

$$\mathbf{K}_{\text{const}} = \mathbf{G}^* \mathbf{V}^* \mathbf{C}^* \mathbf{C} \mathbf{V} \mathbf{G} = \mathbf{B}^* \mathbf{M} \mathbf{A} \mathbf{M}^* \mathbf{B}$$

where we used the definition of \mathbf{G} from (12), $\mathbf{M} = \mathbf{F} \mathbf{U}$, the eigendecomposition of \mathbf{P} from (20) and the QR decomposition $\mathbf{H}_d^* = \mathbf{F} \mathbf{C}$.

converge to zero as well at the same rate [22]. Substituting these back into (32), we obtain:

$$\begin{aligned} & \|\Delta\|_F \|(\mathbf{A}(P) + \Delta(P))^{-1}\|_F \\ &= O(\sqrt{P}P^{-1} \|(\rho\mathbf{K}_{\text{const}} + O(P^{-1/2})\mathbf{I})^{-1}\|_F) \\ &= O(P^{-1/2}) = o(1) \end{aligned} \quad (33)$$

We thus conclude from (33) and the lower bound (28) that choosing $\epsilon(P) = \|\Delta(P)\|_F \|(\mathbf{A}(P) + \Delta(P))^{-1}\|_F \log(e)$ yields the desired lower bound since $\epsilon(P)$ converges to zero and $\beta(P) \geq -\epsilon(P)$. The proof is complete. ■

APPENDIX E PROOF OF THEOREM 2

Proof: Let $R_{s,G}^P$ denote the achievable rate assuming perfect CSI and $R_{s,G}^Q$ denote the achievable rate under the quantized CSI communication scheme.

The first part of the Theorem will be proven first. With perfect CSI, a similar argument as the one presented in Theorem 1 can be used to show:

$$\frac{R_{s,G}^P}{\log P} \xrightarrow{P \rightarrow \infty} d_s \quad (34)$$

Of course, the fact that $\mathbf{G}^*\mathbf{G}$ is full rank (a.s.) is also used.

Define the secrecy rate difference:

$$\begin{aligned} \Delta R_{s,G} &:= R_{s,G}^P - R_{s,G}^Q \\ &= T_+^P - T_-^P - T_+^Q + T_-^Q \end{aligned} \quad (35)$$

where the terms $T_+^P, T_-^P, T_+^Q, T_-^Q$ are defined in (15) and (16). We note that the term $-T_-^P + T_-^Q$ is asymptotically negligible since $-T_-^P + T_-^Q = o(1)$ as $P \rightarrow \infty$. To see this, note:

$$\begin{aligned} T_-^P &= \log \det \left(\mathbf{I} + \frac{\rho}{n_r} \mathbf{H}_e \mathbf{W}_1 \mathbf{W}_1^* \mathbf{H}_e^* \right) \\ &\quad \times \left(\frac{1-\rho}{n_t - n_r} \mathbf{H}_e \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_e^* + \frac{\bar{\sigma}^2}{P} \mathbf{I}_{n_e} \right)^{-1} \\ &\xrightarrow{P \rightarrow \infty} \log \det \left(\mathbf{I} + \frac{\rho}{1-\rho} \frac{n_t - n_r}{n_r} \mathbf{H}_e \mathbf{W}_1 \mathbf{W}_1^* \mathbf{H}_e^* \right. \\ &\quad \left. \times (\mathbf{H}_e \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_e^*)^{-1} \right) =: t_\infty \end{aligned}$$

where we used the condition $n_e \leq n_t - n_r$, implying that $\mathbf{H}_e \mathbf{W}_2 \mathbf{W}_2^* \mathbf{H}_e^*$ is invertible. Using the fact that $\lim_{P \rightarrow \infty} N_f = \infty$, it follows that $\mathbf{W}_{1,Q} \rightarrow \mathbf{W}_1$ and $\mathbf{W}_{2,Q} \rightarrow \mathbf{W}_2$ as the loss due to quantization becomes asymptotically negligible. Therefore, using a similar technique and taking the limit as $P \rightarrow \infty$, it follows that $T_-^Q \rightarrow t_\infty$. Thus, we have $-T_-^P + T_-^Q \rightarrow -t_\infty + t_\infty = 0$. Using this in (35), we obtain:

$$\Delta R_{s,G} = T_+^P - T_+^Q + o(1) \quad (36)$$

Without loss of generality, let us assume $\mathbf{K}_{x_s} \sim cP\mathbf{I}$ for the purposes of analysis since $c_0P\mathbf{I} \preceq \mathbf{K}_{x_s} \preceq c_1P\mathbf{I}$. Using the

definitions of T_+^P and T_+^Q , after some algebra, we obtain:

$$\begin{aligned} \Delta R_{s,G} &\sim \log \det \left(\underbrace{\frac{(1-\rho)P}{n_t - n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G}}_{\mathbf{M}_2(P)} + \sigma^2 \mathbf{G}^* \mathbf{G} \right) \\ &\quad - \log \det(\sigma^2 \mathbf{G}^* \mathbf{G}) \\ &\quad - \left[\log \det \left(\rho P \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{1,Q} \mathbf{W}_{1,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} \right. \right. \\ &\quad \left. \left. + (1-\rho) \frac{P}{n_t - n_r} \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G} \right) \right. \\ &\quad \left. - \log \det \left(\rho P \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{1,Q} \mathbf{W}_{1,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G} + \sigma^2 \mathbf{G}^* \mathbf{G} \right) \right] \\ &\quad + o(1) \end{aligned}$$

The term in the brackets is exactly the remainder term $\beta(P)$ defined in Lemma 4. Using the result of Lemma 4, there exists a sequence $\epsilon(P)$ converging to zero such that:

$$\begin{aligned} \Delta R_{s,G} &\sim \log \det (\mathbf{M}_2(P) + \sigma^2 \mathbf{G}^* \mathbf{G}) \\ &\quad - \log \det(\sigma^2 \mathbf{G}^* \mathbf{G}) - \beta(P) + o(1) \\ &\leq d_s \log(\|\mathbf{M}_2(P) + \sigma^2 \mathbf{G}^* \mathbf{G}\|_2) \\ &\quad - d_s \log(\sigma^2 \lambda_{\min}(\mathbf{G}^* \mathbf{G})) + \epsilon(P) + o(1) \\ &\leq d_s \log \left(\underbrace{\frac{\lambda_{\max}(\mathbf{G}^* \mathbf{G})}{\lambda_{\min}(\mathbf{G}^* \mathbf{G})}}_{\kappa(\mathbf{G}^* \mathbf{G})} + \frac{\|\mathbf{M}_2(P)\|_2}{\sigma^2 \lambda_{\min}(\mathbf{G}^* \mathbf{G})} \right) + \epsilon(P) + o(1) \\ &\leq d_s \log \left(\kappa(\mathbf{G}^* \mathbf{G}) + \frac{(1-\rho)P \|\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V}\|_F^2}{\sigma^2 \lambda_{\min}(\mathbf{G}^* \mathbf{G})} \right) \\ &\quad + \epsilon(P) + o(1) \end{aligned} \quad (37)$$

The term given by $P \|\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V}\|_F^2$ is $O(1)$ as $P \rightarrow \infty$, as the bounds in (31) show. Thus, dividing both sides of (37) by $\log P$ and taking the limit as $P \rightarrow \infty$, we obtain:

$$\begin{aligned} d_s^Q &:= \lim_{P \rightarrow \infty} \frac{R_{s,G}^Q}{\log P} \\ &\geq \lim_{P \rightarrow \infty} \frac{R_{s,G}^P}{\log P} - \lim_{P \rightarrow \infty} \frac{d_s \log(\kappa(\mathbf{G}^* \mathbf{G}) + O(1)) + \epsilon(P) + o(1)}{\log P} \\ &= d_s - 0 = d_s \end{aligned}$$

where we used (34). Since the rate of the quantized CSI scheme is less than the rate of the perfect CSI scheme, it follows that $d_s^Q \leq d_s$. Thus, we conclude that $d_s^Q = d_s$.

The second part of the Theorem now easily follows. Note that from (36), we have:

$$\begin{aligned} \delta_{\text{GAP}} &= \lim_{P \rightarrow \infty} \{R_{s,G}^P - R_{s,G}^Q\} \\ &= \lim_{P \rightarrow \infty} \{T_+^P - T_+^Q\} \\ &\leq \lim_{P \rightarrow \infty} \log \det \left(\mathbf{I} + \frac{(1-\rho)}{\sigma^2} \mathbf{U}(P) (\mathbf{G}^* \mathbf{G})^{-1} \right) \end{aligned} \quad (38)$$

where

$$\mathbf{U}(P) := P \mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q} \mathbf{W}_{2,Q}^* \mathbf{H}_d^* \mathbf{V} \mathbf{G}$$

is a positive semidefinite matrix depending on P . From the development in (31), using the scaling in (17), we obtain:

$$\begin{aligned} \text{tr}(\mathbf{U}(P)) &= P \|\mathbf{G}^* \mathbf{V}^* \mathbf{H}_d \mathbf{W}_{2,Q}\|_F^2 \\ &\leq 2P d_c(\mathbf{F}, \hat{\mathbf{F}})^2 \\ &\leq \frac{8P}{c^{2/N}} 2^{-2N_f/N} (1 + o(2^{-\frac{N_f}{N}})) \Bigg|_{N_f = \frac{(1+\epsilon)N}{2} \log_2 P} \\ &= O(P^{-\epsilon}) \end{aligned}$$

As a result, $\text{tr}(\mathbf{U}(P)) = o(1)$, implying $\mathbf{U}(P) \rightarrow \mathbf{0}$ as $P \rightarrow \infty$ [22]. Using this result in (38), we have $\delta_{\text{GAP}} \leq 0$. The final result following by noting that δ_{GAP} is always nonnegative. The proof is complete. ■

REFERENCES

- [1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, January 1975.
- [2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [4] A. Khisti and G. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, p. 30883104, July 2010.
- [5] —, "Secure transmission with multiple antennas ii: The mimome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, p. 55155532, November 2010.
- [6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, p. 21802189, June 2008.
- [7] N. Jindal, "Mimo Broadcast Channels with Finite-Rate Feedback," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 5045–5060, November 2006.
- [8] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 7, pp. 1478–1491, 2007.
- [9] M. Rezaee and M. Guillaud, "Limited feedback for interference alignment in the K-user MIMO interference channel," in *IEEE Information Theory Workshop (ITW)*, Lausanne, Switzerland, September 2012.
- [10] —, "Interference Alignment with Quantized Grassmannian Feedback in the K-user constant MIMO Interference Channel," *arXiv: 1207.6902*, January 2013.
- [11] R. T. Krishnamachari and M. K. Varanasi, "Interference Alignment under Limited Feedback for MIMO Interference Channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 15, August 2013.
- [12] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, p. 38313842, October 2010.
- [13] X. Zhang, X. Zhou, and M. R. McKay, "On the design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, p. June, 2013.
- [14] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, March 2011.
- [15] A. Mukherjee and A. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, January 2011.
- [16] S. Yang, M. Kobayashi, P. Piantanida, and S. S. (Shitz), "Secrecy Degrees of Freedom of MIMO Broadcast Channels with Delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5244–5256, September 2013.
- [17] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, August 2011.
- [18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.
- [19] D. P. Bertsekas, *Nonlinear Programming*, 2nd ed. Athena Scientific, 1999.
- [20] R. T. Krishnamachari, "A Geometric Framework for Analyzing the Performance of Multiple-Antenna Systems under Finite-Rate Feedback," Ph.D. dissertation, University of Colorado, Boulder, 2011.
- [21] W. Dai, Y. Liu, and B. Rider, "Quantization bounds on Grassmann manifolds and applications to MIMO communications," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1108–1123, March 2008.
- [22] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.